(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 17 900 A1**

(51) Int. Cl.[6]:
G 06 F 12/14
G 06 F 15/167
H 04 L 9/28

(21) Aktenzeichen: 197 17 900.2
(22) Anmeldetag: 28. 4. 97
(43) Offenlegungstag: 30. 10. 97

DE 197 17 900 A1

(30) Unionspriorität:
638807 29.04.96 US

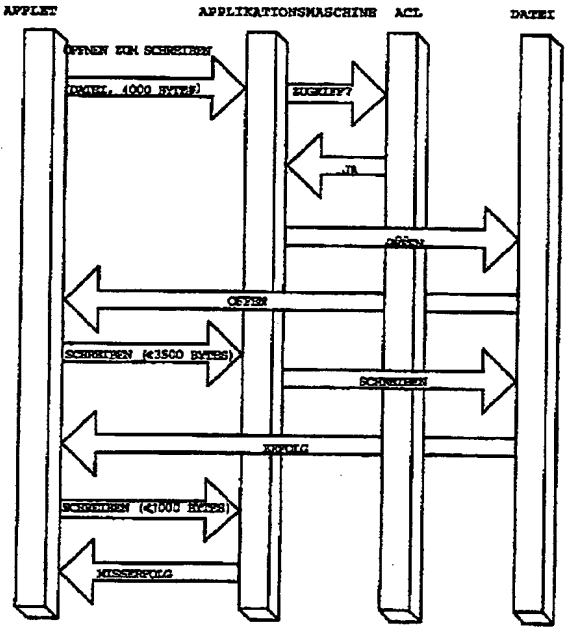
(71) Anmelder:
Mitel Corp., Kanata, Ontario, CA

(74) Vertreter:
PAe Reinhard, Skuhra, Weise & Partner, 80801 München

(72) Erfinder:
Deadman, Richard, Ottawa, Ontario, CA

(54) Verfahren und Vorrichtung zur Verarbeitung eines Computer-Applets

(57) Ein Verfahren zur Verarbeitung eines Applet wird bereitgestellt, welches folgende Schritte aufweist: Speichern einer Datei in einem dauerhaften Speichermedium (PSM), wobei die Datei eine Zugriffskontrolliste aufweist, Übertragen eines Applet von einem Server, wobei das Applet zumindest eines von Applet-Identifizierungsdaten und einem Paar von einem Privatschlüssel-verschlüsselten Domänenidentifizierer und einem Allgemeinschlüssel, einem Dateimaximalgrößen-Indikator und einer Spezifizierung erforderlicher Operationen aufweist, Empfangen des Applets durch eine Applikationsmaschine, im Fall, daß der Domänenidentifizierer im Applet enthalten ist, Entschlüsseln des Domänenidentifizierers unter Benutzung des Allgemeinschlüssels, Prüfen von dem zumindest einen von den Applet-Identifizierungsdaten und dem entschlüsselten Domänenidentifizierer gegenüber der Zugriffskontrolliste nach einer Übereinstimmung, und im Fall, daß eine Übereinstimmung gefunden ist, Ermöglichen der in dem Applet spezifizierten Operationen an einer Datei, die in einem dauerhaften Speichermedium gespeichert ist, für welche ein Zugriff auf das Applet, wie in der Dateizugriffskontrolliste spezifiziert, möglich ist.



DE 197 17 900 A1

Beschreibung

Die vorliegende Erfindung betrifft das Gebiet der Computernetzwerke, und insbesondere ein Verfahren zum Verarbeiten von Computer-Applets auf sichere Art und Weise.

Mit dem Aufkommen des objektbasierenden bzw. objektorientierten Programmierens wurde es möglich, Applets über ein Netzwerk, wie z. B. das Internet, an verschiedene, mit dem Netzwerk verbundene Computer zu übertragen. Ein Applet ist ein kleines, unabhängiges Anwendungsprogramm bzw. Applikationsprogramm, das einen Computer veranlassen kann, eine bestimmte Funktion aus zuführen, und sowohl Anweisungen für den Betrieb des Computers als auch Daten, welche bei seinem Betrieb zu verarbeiten sind, enthält.

Verschiedene Programmiersprachen wurden zur Erstellung von Applets entworfen, wie z. B. Telescript, SafeTCL, Java, Cyber-Agents und ClearLake Agents. Durch Benutzung von Interpretierern können die verschiedenen Applets Hardware-unabhängig sein, d. h. dasselbe Applet kann von Computerhardware mit verschiedenen Betriebssystemen empfangen und verarbeitet werden. Beispielsweise wäre es möglich, daß dasselbe Applet von einem MacIntosh-Betriebssystem empfangen und verarbeitet wird sowie von einem der Microsoft Windows-Betriebssysteme auf Personalcomputer-Betriebssystemen, basierend auf einem Intel-Prozessor (z. B. IBM).

Man hat spekuliert, daß die Programme und Daten, welche Computer, die Applets empfangen, benutzen, all das bereitstellen würden, was ein Computer braucht, um in der Lage zu sein, vollständig zu funktionieren, was in einem signifikant weniger kostenträchtigen Computer als gegenwärtig resultieren würde. Dies kommt daher, daß der Computer erwartungsgemäß das Netzwerk als Massenspeicher-Ablage von Programmen und Daten benutzen würde. Programme würden auf einer Benutzungsbasis bezahlt werden, und nicht auf einer Vorauszahlungsbasis und einer Basis der unbeschränkten Benutzung. Jedoch setzt dies voraus, daß ein Benutzer darauf vorbereitet wäre, zu erlauben, daß eine Massenspeicherung zur Speicherung kritischer Daten, insbesondere geschriebener Programme usw. außerhalb seiner Kontrolle wäre. Aus Sicherheitsgründen, glaubt man, ist es wünschenswert und/oder notwendig, einen lokalen Massenspeicher in Zusammenhang mit jedem oder mit den meisten Computern bereitzustellen.

Bei der Speicherung von Daten auf einer lokalen Massenspeichervorrichtung entsteht das Problem der Sicherheit in bezug auf den Empfang der Applets vom Netzwerk, da diese Applets auf Dateien zugreifen, diese übertragen oder beschädigen könnten.

Das Sicherheitsproblem wurde bisher auf eine von zwei Arten gehandhabt.

Die erste besteht in der Beschränkung der Benutzung der Applets auf ein geschlossenes oder verwaltetes System, wobei Softwarekomponenten Domänennamen erhalten können und alle möglichen Ausführungsplätze mit Listen erlaubter Domänen bestückt werden können. Beispielsweise werden im CyberAgents-Programm Domänen zur Steuerung der Ausführung und der Sicherheit an entfernt gelegenen Plätzen benutzt. Eine Domäne ist eine Gerichtsbarkeitsgruppe von Applets, welche sich Zugriffsrechte teilen.

Der zweite Weg der Handhabung der Sicherheit besteht in der Isolierung der Applets von wichtigen Systemressourcen, wie weiter oben bemerkt. Von einem unkontrollierten Systemnetzwerk, wie z. B. dem Internet, empfangene Applets wurden am Zugriff auf Massenspeichervorrichtungen gehindert und wurden zur Bereitstellung fantasievoller Graphiken und zur Bereitstellung einer graphischen Benutzerschnittstelle für das Kunden-Server-Computing umgeleitet. Programme zur Erzeugung von Applets in offenen unkontrollierten Systemen sind beispielsweise Telescript, SafeTCL und Java. Beispielsweise kann Java einen Computer veranlassen, ein Fenster anzuzeigen und den Inhalt des Fensters bereitstellen sowie Klänge zu spielen, aber es kann nicht auf das Computer-Plattenlaufwerk schreiben.

Obwohl die Benutzung von irgendeinem dieser Schemen die Sicherheit hervorbringt, welche erforderlich ist, zu gewährleisten, daß Gauner-Applets keinen Schaden an den Ressourcen eines Computers anrichten, wie z. B. an den Dateien, erlegen sie ebenfalls der Benutzbarkeit von mobilen Applets eines offenen Systems eine Beschränkung auf. Falls ein heruntergeladenes Applet keinen Zugriff auf das Plattenlaufwerk hat, um eine dauerhafte lokale Speicherung für den Benutzer zu erzeugen, ist die Benutzbarkeit von geschriebenen Applets, die solch ein Isolierungsschema benutzen, sehr beschränkt.

Betriebssysteme kümmern sich um die Sicherheit durch Bereitstellung von Benutzungsrechten für Verzeichnisse und Dateien. Durch Zuordnung der Applet-Applikationsmaschine zu einer Benutzergruppe werden die durch die Applikationsmaschine ausgeführten Applets darauf beschränkt, auf die Dateien zuzugreifen, die in der Applikationsmaschine selbst verfügbar sind.

Obwohl dies Sicherheit für weitere Dateisystem-Dateien außerhalb des Einflußgebiets der Applikationsmaschine bietet, bietet es keine Sicherheit zwischen den Applets. In ähnlicher Weise bieten manche Applet-Applikationsmaschinen, wie z. B. HotJava von Sun, Zugriffskontrollisten. Diese Listen spezifizieren, welcher Untersatz der zugriffsfähigen Dateien der Applikationsmaschinen einen Zugriff durch Applets erfahren kann. Dies bietet eine ausgedehnte Sicherheit, löst aber nicht das Problem der Bereitstellung der Sicherheit für Daten zwischen Applets.

HotJava spezifiziert ebenfalls ein Verfahren, durch das ein Zugriff auf Dateien für Applets durch Benutzung einer Dialogbox für den Benutzer des Applet ermöglicht werden kann, wobei der Benutzer eine Sicherheitsautorisierung bzw. -berechtigung eingeben muß. Dies bietet eine größere Sicherheit zwischen den Applets, ist aber intrusiv und erfordert, daß der Benutzer die Empfindlichkeit und den Ursprung (virtuelle Inhaberschaft) der Daten in jeder Datei versteht.

Falls die Applikationsmaschine die Quelle des Applets bestimmen kann, können Zugriffsrechte gemäß bestimmten Regeln eingerichtet werden. Java kann erfassen, ob ein Applet von innerhalb einer Feuerwand bzw. "Firewall" (einer Softwarebarriere zu einem Außenzugriff auf ein lokales (internes) Netzwerk) herrührt; der HotJava-Browser ermöglicht verschiedene Sicherheitsrechte für Applets, die auf jeder Seite der Feuerwand

geladen werden. Lese- und Schreibzugriff kann nur internen Applikationen gewährt werden.

General Magic's Telescript-Technologie bietet einen generischen Satz von Berechtigungen und Zulassungen. Agenten innerhalb eines Bereichs enthalten alle dieselbe Berechtigung — dies ist ähnlich wie das Konzept der Benutzerdomänen. Jeder Telescript-Agent hat nur eine Berechtigung. Zulassungen kontrollieren die Ausführung von Anweisungen oder den Zugriff und die Benutzung einer Ressource. Telescript spezifiziert nicht, wie ein Telescript-Ort über Benutzungsrechte für eine Ressource mit einem Agenten einer bestimmten Berechtigung verhandelt oder die Zugriffsrechte für jede Ressourceninstanz speichert.

Der Ausdruck "dauerhafte Speicherung" wird in dieser Beschreibung als generischer Ausdruck für alle Medien benutzt, welche Dateien, Daten oder Programme, welche zu schützen sind, speichern oder tragen und kann elektronische Schreib-/Lesespeicher, Floppy- oder Festplattenlaufwerke, Busse usw. umfassen, ist aber nicht darauf beschränkt.

Die vorliegende Erfindung schafft einen sicheren Zugriff auf einen dauerhaften Speicher für einen verteilten Applet-Code innerhalb einer offenen, unkontrollierten Computing-Umgebung. Sie schützt Dateien vor unberechtigter Benutzung durch unbekannte mobile Applets, wobei sie noch Zugriff auf das Datei-System für diese Applets bietet. Dies involviert die Verhandlung von Zugriffsrechten für das unbekannte Applet.

In Übereinstimmung mit einer Ausführungsform der Erfindung umfaßt ein Verfahren zur Verarbeitung eines Applet die Speicherung einer Datei in einem dauerhaften Speichermedium (PSM), wobei die Datei eine Zugriffskontrolliste aufweist, und die Übertragung eines Applet von einem Server, wobei das Applet zumindest eines von Applet-Identifizierungsdaten und einem Paar aus Privatschlüssel-kodiertem Domänenidentifizierer und Allgemeinschlüssel, einem Dateimaximalgrößen-Indikator und einer Spezifikation erforderlicher Speicheroperationen enthält, den Empfang des Applet durch eine Applikationsmaschine, und im Fall, daß der Domänenidentifizierer im Applet enthalten ist, das Entschlüsseln des Domänenidentifizierers unter Benutzung des Allgemeinschlüssels, das Prüfen von zumindest einem von den Applet-Identifizierungsdaten und dem entschlüsselten Domänenidentifizierers gegenüber der Zugriffskontrolliste hinsichtlich einer Übereinstimmung, und im Fall, daß eine Übereinstimmung gefunden wird, das Ermöglichen der in dem Applet spezifizierten Operationen an einer in einem dauerhaften Speichermedium gespeicherten Datei, für welche ein Zugriff für das Applet, wie in der Dateizugriffskontrolliste spezifiziert, möglich ist.

In Übereinstimmung mit einer weiteren Ausführungsform umfaßt ein Verfahren zur Verarbeitung eines Applet den Empfang von Applets in einer Applikationsmaschine, wobei die Applets Spezifikationen von durchzuführenden Operationen aufweisen und einige der Applets zumindest eines von Applet-Identifizierungsdaten und Privatschlüssel-verschlüsselten Domänen aufweisen, Verarbeiten der Applets in einem Ausmaß, in dem ein Zugriff auf in einem dauerhaften Speichermedium enthaltene Dateien nicht erforderlich ist, in dem Fall, daß die Applets Privatschlüssel-verschlüsselte Domänen aufweisen, Entschlüsseln der Domänen, Prüfen von zumindest einem der Applet-Identifizierungsdaten und der entschlüsselten Domänen gegenüber einer Kontrolliste, und Verarbeiten der Applets, von denen das zumindest eine von Applet-Identifizierungsdaten und entschlüsselten Domänen mit Einträgen in der Kontrolliste zum Zugriff auf die im dauerhaften Speichermedium enthaltenen Dateien übereinstimmt, wie durch die Applets gefordert.

In Übereinstimmung mit einer weiteren Ausführungsform umfaßt ein Verfahren zur Verarbeitung eines Applet das Speichern einer Zugriffskontrolliste, welche eine Identität von Applets oder Domänen enthält, die einen Zugriff auf in einem dauerhaften Medium gespeicherte Dateien haben können, und Ermöglichen des Zugriffs auf das Zugriffskontrollmedium durch die Applets, welche eine Identität oder eine Domäne entsprechend einem Eintrag auf der Liste aufweisen.

In Übereinstimmung mit einer weiteren Ausführungsform umfaßt eine Applet-Applikationsmaschine aus einer Zugriffskontrolliste, wobei die Maschine und die Liste in einem Speicher eines Computers gespeichert sind, und eine Vorrichtung zum Bereitstellen eines Applet mit einer Identifizierung mit zumindest einem von einem Applet-Identifizier und einer Domäne zum Vergleich mit der Liste und zur Bestimmung einer Übereinstimmung, sowie eine Vorrichtung zur Ermöglichung eines Zugriffs auf eine anderenfalls geschützte Computerressource im Fall der Übereinstimmung.

Ein besseres Verständnis der Erfindung wird durch Betrachtung der nachstehenden detaillierten Beschreibung mit Bezug auf die begleitenden Zeichnungen erhalten.

Es zeigen:

Fig. 1 ein Blockdiagramm eines Netzwerks, auf dem die vorliegende Erfindung implementiert werden kann;

Fig. 2 ein Blockdiagramm eines in dem Netzwerk von Fig. 1 benutzten Computers, auf dem die vorliegende Erfindung implementiert werden kann;

Fig. 3 eine Illustration eines repräsentativen Applets, welches bei der vorliegenden Erfindung benutzt wird; und

Fig. 4 ein repräsentatives Betriebsverfahren nach der vorliegenden Erfindung.

Fig. 1 illustriert ein offenes und unkontrolliertes Netzwerk und umfaßt einem Server 1, welcher eine Schnittstelle zu einem Netzwerk 3 aufweist, mit dem verschiedene Computer 5 verbunden sind oder verbunden werden können. Das Netzwerk 3 kann ein Großbereichsnetzwerk, das Internet, ein Telefonnetzwerk usw. sein.

Im Betrieb liefert der Server 1 Applets an das Netzwerk 3 zum Empfang durch einen oder mehrere Computer 5. Ein Computer, der das Applet empfängt, das ein vollständiges objektbasierendes Programm ist, verarbeitet es unter Benutzung der darin enthaltenen Daten. Wie oben erwähnt, war bei offenen Systemen nach dem Stand der Technik das Applet daran gehindert, einen Zugriff auf einen dauerhaften Speicher auszuüben.

Fig. 2 illustriert die grundlegende Architektur eines repräsentativen Computersystems 5. Ein Mikroprozessor 7, ein Schreib-/Lesespeicher 8 (RAM), eine Tastatur 9, eine Netzwerk-Schnittstellenvorrichtung 10, wie z. B. ein Modem, eine dauerhafte Speichervorrichtung in Form eines Festplattenlaufwerks 11 sowie ein Anzeigeuntersystem 12, mit der eine Anzeige 13 verbunden ist, sind mit einem Bus 14 verbunden oder stehen in Kommunikation

damit.

Zusätzlich ist der Schreib-/Lesespeicher 16 (RAM), der ein Teil des RAM 8 sein kann oder darin enthalten sein kann, mit dem Bus 14 verbunden oder steht in Kommunikation damit. Der RAM 16 enthält eine Applet-Applikationsmaschine, die einen Interpretierer für die bestimmte benutzte Applet-Sprache und eine Software-Befehlsstruktur zur Veranlassung des Mikroprozessors 7, die Applets zu verarbeiten, aufweist. Beispielsweise kann für die Java-Sprache eine Applet-Applikationsmaschine eine HotJava sein, die von Sun Microsystems Inc. erhältlich ist.

Beim Betrieb eines Systems nach dem Stand der Technik werden Applets von dem Server 1 über das Netzwerk 3 und die Netzwerkschnittstelle 10 empfangen und werden von dem Mikroprozessor 7 unter Benutzung des Interpretierers in der Anwendungsmaschine 16 interpretiert, und die interpretierten Anweisungen werden durch den Mikroprozessor 7 verarbeitet, um zu veranlassen, daß das Anzeigeuntersystem 12 Graphiken usw. auf der Anzeige 13 anzeigt. Die Applikationsmaschine hat keinen Zugriff auf dauerhafte Speichermedien, wie z. B. das Festplattenlaufwerk 11, um eine Beschädigung usw. der Dateien, wie beschrieben, zu vermeiden, und deshalb kann sie darin gespeicherte Benutzerdaten oder weitere Programme nicht benutzen. Solch ein System ist beträchtlich eingeschränkt.

In Übereinstimmung mit der vorliegenden Erfindung enthält die Applikationsmaschine 16 ein Allgemeinschlüssel-Entschlüsselungsprogramm 18 sowie eine Zugriffskontrolliste 20 berechtigter Applets und/oder Domänen, welche eine Erlaubnis erhalten können, auf dauerhafte Speichermedien zuzugreifen.

In Übereinstimmung mit der vorliegenden Erfindung werden, wenn Applets über die Netzwerkschnittstelle empfangen werden, Zugriffsrechte auf die dauerhaften Speichermedien unter Benutzung der Applikationsmaschine 16 verhandelt. Die Zugriffsrechte brauchen nicht beschränkt zu werden, und der Zugriff muß nicht nur hinsichtlich dauerhafter Speichermedien verhandelt werden; jegliche Ressource des Computers oder jegliche vom Computer gesteuerte oder zum Zugriff verfügbare Ressource kann beschränkt werden, und über ein Zugriff darauf kann verhandelt werden.

Die Zugriffsrechte werden verhandelt durch:

(a) Berechtigung; die Applet-Applikationsmaschine verifiziert die Identität oder die Domäne aller Applets, welche einen Zugriff auf den dauerhaften Speicher fordern;

(b) Benutzungsrechte-Verhandlung; dies involviert die Verifizierung der Berechtigung des Applet, zu lesen, zu schreiben oder einen Zusatz an eine Datei zu bilden. Verfahren zur Gewährleistung, daß ein Applet Zugriffsrechte auf eine bestimmte Datei hat, werden nachstehend beschrieben. Es sollte bemerkt werden, daß in einem offenen unkontrollierten System eine zentrale Berechtigungs- oder Domänenverwaltung nicht möglich ist. Aus diesem Grund wird die Verhandlung über die Zugriffsrechte zwischen der Applikationsmaschine, der Datei und dem Applet durchgeführt;

(c) Servicequalität; eine maximale Plattenbenutzung für eine Applikation wird eingestellt. Grenzen werden den Zugriffsrechten vorzugsweise auferlegt, welche Schranken angeben, innerhalb denen die gewährte Ressource benutzt werden kann.

Durch Wirkung als Vermittler zwischen einem unbekannten Applet und der Plattenressource verhandelt die Applikationsmaschine und setzt Zugriffsrechte durch. Für Plattendateien involviert dies die Wirkung als Vermittler für alle Plattenaktionen. Wenn eine Zieldatei über eine vorbestimmte Größe hinaus anwächst, kann ein Schreibzugriff verneint werden, oder der Benutzer kann nach der Erlaubnis zum Überschreiben gefragt werden, was effektiv ein Wachstum der Zugriffsrechte um einen inkrementierten Betrag ermöglicht. Die Applikationsmaschine kann eine Überschreibzone definieren, über die hinaus das Zugriffsrecht nicht anwachsen darf.

Als ein Sicherheitsmechanismus kann eine Datei-Versionsverwaltung durch die Applikationsmaschine vorgesehen werden, um zu gewährleisten, daß irgendwelche Modifikationen oder Löschungen an den Dateien im Fall der Beschädigung des Dateisystems behebbar sind. Die Zugriffskontrolliste 20 wird durch die Applikationsmaschine benutzt, um zu spezifizieren, welche vorgegebenen und dateispezifischen Zugriffsrechte für individuelle dauerhafte Speicherobjekte (Dateien) vorliegen.

Jedem Applet sollte ein Server-Platz zugeordnet sein, der das Applet eindeutig identifiziert. Falls beispielsweise von World Wide Web geladen, kann diese Identität der universelle Ressourcen-Lokalisierer (URL) des Applet sein. Wenn ein Applet eine neue Datei erzeugt, kann es spezifizieren, welche Applets Rechte an der Datei besitzen.

Domänen sind Gruppen von Applets, welche Zugriffsrechte teilen. Unter Benutzung von einer Privatschlüssel-Verschlüsselung und einer vom Applet zugeführten verschlüsselten Nachricht kann die Applikationsmaschine gewährleisten, daß ein Applet zu einer spezifizierten Domäne gehört. Applet-Dateien enthalten einen Vorsatz, welcher die Zugriffskontrolliste für einen Satz von Domänen und die Allgemeinschlüssel für jede Domäne enthält.

Fig. 3 illustriert ein Applet 22, welches eine Nutzlast 24 bestehend aus einem objektbasierendem Anwendungsprogramm einschließlich Daten, sowie einen Vorsatz 26 enthält. Der Vorsatz 26 enthält einen Allgemeinschlüssel oder mehrere Allgemeinschlüssel 28 sowie eine Applikationskontrolliste 30. Er enthält ebenfalls eine Identifizierung des Applets (z. B. den URL, falls bei World Wide Web benutzt), welche am Server unter Benutzung eines Privatschlüssels verschlüsselt werden kann, zur Entschlüsselung unter der Steuerung der Applikationsmaschine 16 unter Benutzung eines Allgemeinschlüssels 28. Der Vorsatz enthält ebenfalls einen verschlüsselten Satz von Domänen, z. B. Domänennachrichten, welche unter Benutzung eines Allgemeinschlüssels 28 entschlüsselt werden können.

Ein Applet kann gleichzeitig zu einer oder mehreren Domänen gehören. Es ist die Verantwortlichkeit der Domäneninhaber, zu gewährleisten, daß der Privatschlüssel, der zur Erzeugung der verschlüsselten Domäne-

nauthentizitätsnachrichten benutzt wird, geheimgehalten wird.

Wie oben erwähnt, kann die verschlüsselte Nachricht die Applet-Identifizierung unter Benutzung des Privatschlüssels verschlüsseln. Dies gewährleistet, daß die verschlüsselte Nachricht nicht von einem anderen Applet im Versuch, diese Applet-Domänenmöglichkeiten zu borgen, kopiert worden ist. Jeglicher Versuch, das Server-Applet auf eine ändere Maschine zu klonen und dann in der Lage zu sein, die domäneneigenen Dateien zu lesen, würde dann bewirken, daß die verschlüsselte Nachricht nicht mit der Applet-Identifizierung übereinstimmt, und würde die Applet-Domäne innerhalb der Applikationsmaschine ungültig machen.

Eine Kombination von Zugriffsverfahren wird vorzugsweise benutzt, um für Applets einen sicheren Zugriff auf dauerhafte Speicher vorzusehen. Sowohl die Applet-Identifizierung als auch vorzugsweise die Domänen werden als Schlüssel innerhalb der Zugriffskontrolliste für eine Datei implementiert.

Die Sprachenklassen zum Dateizugriff in der Applikationsmaschine **16** für die bestimmte benutzte Sprache, z. B. Java, sollte verbessert werden, so daß sie einen Zugriff auf das Dateisystem basierend auf der Applet-Identifizierung und der Domäne erlaubt. Applets sollten, wie oben angedeutet bezüglich **Fig. 3**, modifiziert werden, um optionell ihre Domäne zu enthalten, sowie durch die Benutzung einer Allgemeinschlüssel-Verschlüsselung davon und/oder ihrer Identifizierung. Jede Datei mit Zugriffsrechten, die ihr zugeordnet sind, ist in der Zugriffskontrolliste **20** (**Fig. 2**) in einer im RAM **16** gespeicherten Datei, auf die durch die Applikationsmaschine zugegriffen werden kann, z. B. ein Browser-Programm, enthalten. Die Applikationsmaschine, die im RAM **16** enthalten ist, verhandelt Zugriffsrechte für jedes geladene Applet. Zugriffsrechte können Servicequalitätsinformationen enthalten, welche definiert, wie auf jede Ressource zugegriffen werden kann, einschließlich der Maximalgröße von Änderungen. Jede Änderung am Dateisystem wird überprüft, um offenzulegen, ob sie Zugriffsrechte verletzen würde. Dies beinhaltet das Recht auf Zugriff, Änderung oder Schaffung einer Datei und die Grenzen der Größe der Änderungen.

Die Struktur der Zugriffskontrolliste ist vorzugsweise folgende:

```
<Filename:...>
    <<AccessMode,...>:<IDorDomain,...>;...>
```

wobei:
Filename enthält einen oder mehrere Dateinamen, von denen jeder Wild-Cards enthalten kann
AccessMode ist eines von Lesen, Schreiben, Anhängen, Löschen, Neue Datei, Auflisten, Anfragen, (MMaxSize: x)
IDorDomain ist entweder ein URL zum Spezifizieren eines Applet oder ein (DomainName: publicKey)-Paar

Beispielsweise kann ein Eintrag, wo alle Dateien in "/public"-Verzeichnis lesbar sind, "/private" durch das Applet neue Dateien geschaffen bekommen kann, URL "http://www.foo.bar/applet.class" und Applets der Domäne "MyDomain" Schreibzugriff auf die Datei "/private/foo.bar" mit auf 5000 Byte eingestelltem Hinzufügungsmodus haben, vorliegen als:

```
/public/*
    Read : *
/private/*
    New File : *
/private/foo.bar
    Write, (MaxSize:5000) :
http://www.foo.bar/applet.class; (MyDomain: 987654321)
```

Eine innerhalb der Applikationsmaschine gesendete Nachricht würde so, wie im Fließdiagramm von **Fig. 4** gezeigt, in dem die Zeit von der Oberseite zur Unterseite der Figur verläuft, in Erscheinung treten.

In diesem Beispiel fordert das Applet das Öffnen der Datei zum Einschreiben von 4000 Byte an. Die Zugriffskontrolliste (ACL) wird durch die Applikationsmaschine befragt. Die Anforderung wird gebilligt, und die Datei wird geöffnet. Wenn 3500 Byte hinzugefügt werden, hat das Schreiben in die Datei Erfolg. Ein Versuch, weitere 1000 Byte zu schreiben, beschert einen Mißerfolg, und diese werden nicht geschrieben, da sie die gespeicherten Zugriffsrechte (4000 Byte) der Applikationsmaschine für das Applet hinsichtlich der Datei überschreiten.

Somit ist ersichtlich, daß die vorliegende Erfindung ein Verfahren schafft, durch das Applets Zugriff auf Dateien haben können, die auf dauerhaften Speichermedien gespeichert sind, oder Zugriff auf andere Computersystemressourcen in einem offenen System haben können, die anderenfalls geschützt wären, und zwar auf sichere Art und Weise, ohne Besorgnis, daß ein Gauner-Applet die Domäne eines anderen Applet angenommen hat, oder die Besorgnis, daß eine Datei gestohlen oder beschädigt werden kann. Das Verfahren bietet ebenfalls Schutz gegen Überlauf der Speichermedien aufgrund einer Erzeugung von Dateien mit übermäßiger Größe.

Und zur gleichen Zeit erlaubt es eine sophistiziertere Funktionsweise eines Computers, der mit einem offenen System verbunden ist, daß Dateien und weitere Ressourcen, die durch einen lokalen Computer gesteuert werden oder damit verbunden sind, bei der Verarbeitung von Applets benutzt werden können.

Eine Person, die die Erfindung versteht, kann jetzt alternative Strukturen und Ausführungsformen oder Variationen der obigen ersinnen. All diejenigen, welche in den Schutzumfang der hieran angehängten Patentansprüche fallen, sollen Teil der vorliegenden Erfindung sein.

Patentansprüche

1. Verfahren zum Verarbeiten eines Applet mit den Schritten:
(a) Speichern einer Datei in einem dauerhaften Speichermedium (PSM), wobei die Datei eine Zugriffskontrolliste enthält,
(b) Übertragen eines Applets von einem Server, wobei das Applet zumindest eines von Applet-Identifizierungsdaten und eines Paares von einem Privatschlüssel -verschlüsselten Domänenidentifizierer und einem Allgemeinschlüssel, einem Dateimaximalgrößenindikator und einer Spezifizierung erforderlicher Operationen enthält,
(c) Empfangen des Applets durch eine Applikationsmaschine,
(d) im Fall, daß der Domänenidentifizierer im Applet enthalten ist, Entschlüsseln des Domänenidentifizierers unter Benutzung des Allgemeinschlüssels,
(e) Prüfen des zumindest einen von den Applet-Identifizierungsdaten und dem entschlüsselten Domänenidentifizierer gegenüber der Zugriffskontrolliste hinsichtlich einer Übereinstimmung; und
(f) im Fall, daß eine Übereinstimmung gefunden wird, Ermöglichen der in dem Applet spezifizierten Operationen an einer in einem dauerhaften Speichermedium gespeicherten Datei, für welche ein Zugriff für das Applet, wie in der Dateizugriffskontrolliste spezifiziert, möglich ist.

2. Verfahren nach Anspruch 1, gekennzeichnet durch den Schritt der Beendigung der Durchführung der in dem Applet spezifizierten Operation in dem Fall, daß die Operation in einer Dateigröße im dauerhaften Speichermedium resultieren würde, welche die Dateimaximalgröße, die im Applet angezeigt ist, überschreitet.

3. Verfahren nach Anspruch 1, gekennzeichnet durch den Schritt der Nicht-Durchführung der Operation im Fall, daß keine Übereinstimmung gefunden wird.

4. Verfahren zur Verarbeitung von Applets mit den Schritten:
(a) Empfangen von Applets in einer Applikationsmaschine, wobei die Applets Spezifikationen von durchzuführenden Operationen aufweisen und einige der Applets zumindest eines von Applet-Identifizierungsdaten und Privatschlüssel-verschlüsselten Domänen aufweisen,
(b) Verarbeiten der Applets in einem Ausmaß, in dem Zugriff auf in einem dauerhaften Speichermedium enthaltene Dateien nicht erforderlich ist,
(c) im Fall, daß Applets Privatschlüssel-verschlüsselte Domänen aufweisen, Entschlüsseln der Domänen,
(d) Prüfen des zumindest einen von den Applet-Identifizierungsdaten und den entschlüsselten Domänen gegenüber einer Kontrolliste, und
(e) Verarbeiten derjenigen Applets, von denen zumindest das eine von den Applet-Identifizierungsdaten und den entschlüsselten Domänen mit Einträgen in der Kontrolliste zum Zugriff auf die in dem dauerhaften Speichermedium enthaltenen Dateien übereinstimmen, wie durch die Applets gefordert wird.

5. Verfahren zum Verarbeiten eines Applet mit den Schritten Speichern einer Zugriffskontrolliste, welche eine Identität von Applets oder Domänen enthält, die einen Zugriff auf in einem dauerhaften Speichermedium gespeicherte Dateien haben können, und Ermöglichen eines Zugriffs auf das dauerhafte Medium durch Applets, welche eine Identität oder eine Domäne entsprechend einem Eintrag auf der Liste aufweisen.

6. Verfahren nach Anspruch 5, gekennzeichnet durch den Schritt der Benutzung einer in einem Computer gespeicherten Applikationssteuermaschine zur Prüfung der Applets, Prüfung der Zugriffskontrolliste und Verarbeitung der Applets, die auf der Zugriffskontrolliste zur Bearbeitung einer in dem Zugriffssteuermedium gespeicherten Datei identifiziert werden.

7. Verfahren nach Anspruch 6, gekennzeichnet durch den Schritt des Prüfens eines Applet hinsichtlich einer Dateigrößen-Beschränkungsspezifizierung, die von dem Applet getragen wird, und Ablehnen, die Datei zu bearbeiten, wenn die durch das Applet spezifizierte Operation in einer Dateigröße oberhalb der spezifizierten Dateigröße resultieren würde.

8. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß zumindest eines von der Identifizierung und der Domäne, die von dem Applet getragen werden, Privatschlüsselverschlüsselt ist und einen entsprechenden Allgemeinschlüssel aufweist, und mit den Schritten des Entschlüsselns zur Feststellung der Authentizität des zumindest einen von der Identifizierung und der Domäne unter Benutzung des Allgemeinschlüssels, wobei der Schritt der Vergabe eines Zugriffs nur in dem Fall ausgeführt wird, daß das entschlüsseite zumindest eine von der Identifizierung und der Domäne Authentizität aufweist.

9. Applet-Applikationsmaschine mit einer Zugriffssteuerliste, wobei die Maschine und die Liste in einem Speicher eines Computers gespeichert sind, sowie einer Einrichtung zum Bereitstellen eines Applet mit einer Identifizierung und zumindest einem von einem Applet-Identifizierer und einer Domäne zum Vergleich mit der Liste und zur Bestimmung einer Übereinstimmung, sowie einer Einrichtung zur Ermöglichung eines Zugriffs auf eine anderenfalls geschützte Computerressource im Fall der Übereinstimmung.

10. Maschine nach Anspruch 9, dadurch gekennzeichnet, daß die Computerressource ein dauerhaftes

Speichermedium ist.

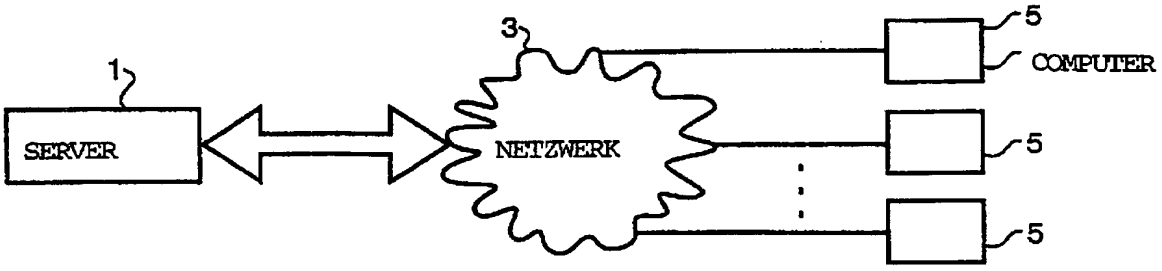
11. Maschine nach Anspruch 9, gekennzeichnet durch eine Allgemeinschlüssel-Entschlüsselungseinrichtung, wobei das Applet einen Privatschlüssel-verschlüsselten Identifizierer oder eine Domäne und einen Allgemeinschlüssel aufweist, zur Entschlüsselung durch die Entschlüsselungseinrichtung.

12. Computersoftware-Applet mit einem Privatschlüsselverschlüsselten Authentizitätscode zum Definieren einer Domäne des Applets.

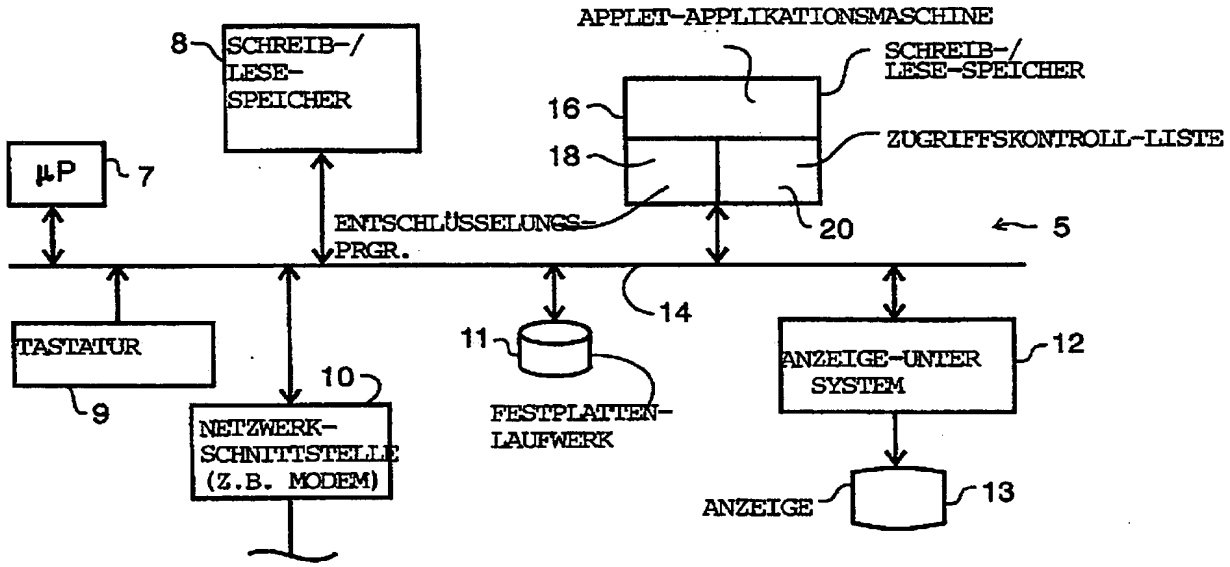
Hierzu 2 Seite(n) Zeichnungen

– Leerseite –

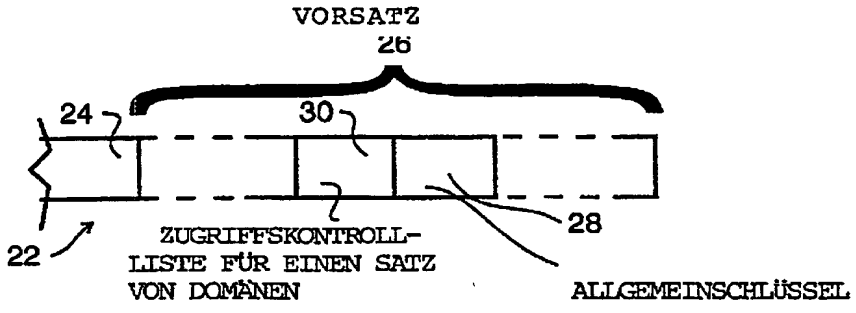
Nummer: DE 197 17 900 A1
Int. Cl.[6]: G 06 F 12/14
Offenlegungstag: 30. Oktober 1997



F I G. 1



F I G. 2



F I G. 3

Nummer: DE 197 17 900 A1
Int. Cl.[8]: G 06 F 12/14
Offenlegungstag: 30. Oktober 1997

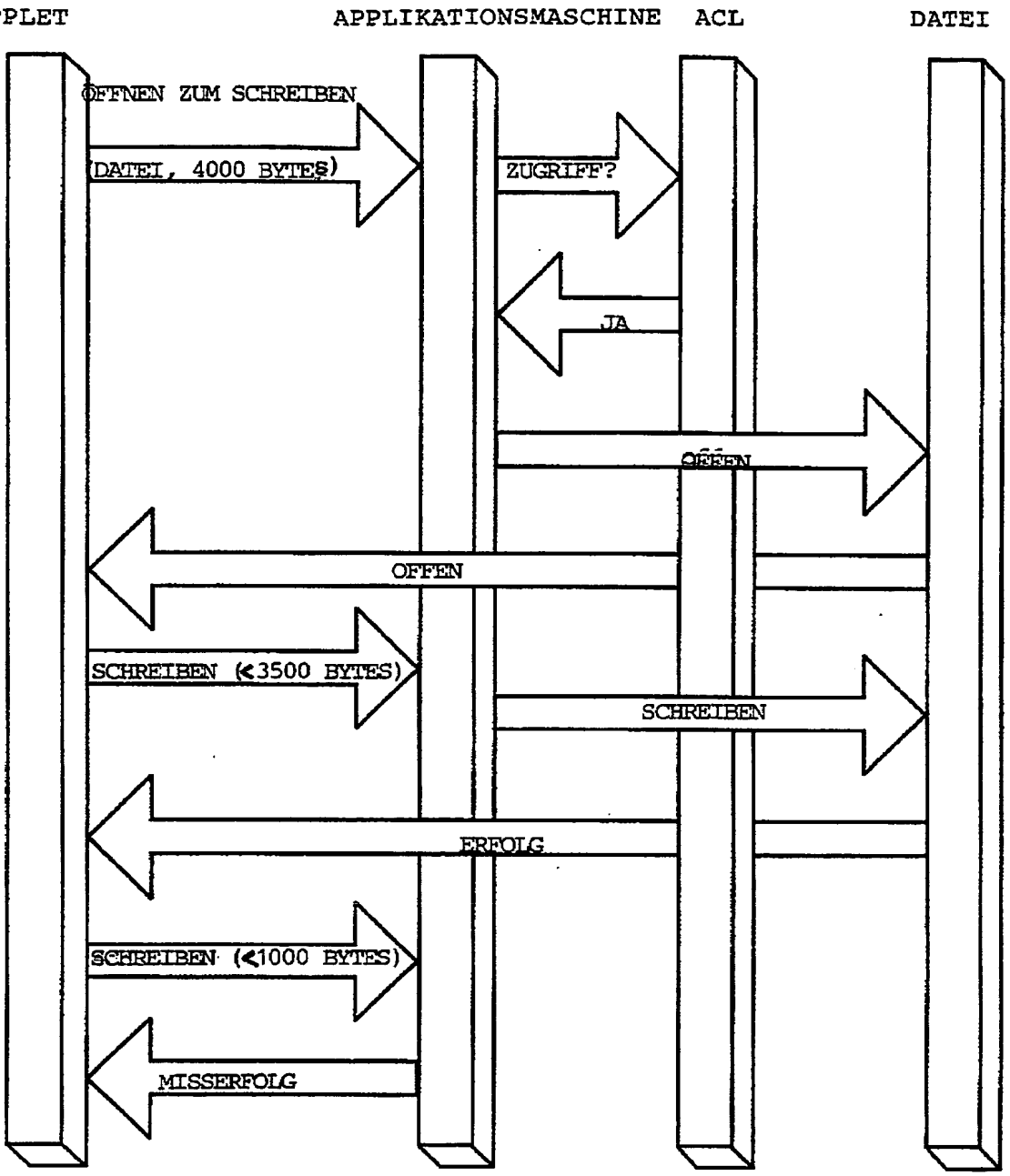


FIG. 4